Requested Patent: JP7244639A

Title: ACCESS RIGHT MANAGEMENT DEVICE ;

Abstracted Patent: JP7244639 ;

Publication Date: 1995-09-19 ;

Inventor(s): OURA MASAHIKO ;

Applicant(s): FUJITSU LTD ;

Application Number: JP19940032713 19940303 ;

Priority Number(s): ;

IPC Classification: G06F15/00 ;

Equivalents: ;

ABSTRACT:

PURPOSE:To flexibly change the right to access and facilitate its management as to access right management for managing the adequacy of a process request in an information system which offers plural information process services to plural users.

CONSTITUTION:The access right management device has a user qualification file 41 which holds records consisting of user IDs and qualification IDs as items, an access right files 42 consisting of service IDs, qualification IDS or user IDs, the kinds of access and whether or not the access is allowed, and the priority of records as items, a request acceptance means 1, an access right determination means 2, an access right holding means 3, and a service start means 5. The access right determination means 2 takes a qualification ID out of the user qualification file 41 based on the user ID as a key, retrieves the access right file 42 based on the qualification ID and the user ID as keys, and determines and holds whether or not final access is allowed with a high-priority record regarding the same service in the access right holding means 3.

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平7－244639

(43)公開日　平成７年(1995)９月19日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　15/00	３３０　Ａ	7459－5Ｌ		

審査請求　未請求　請求項の数３　ＯＬ　（全７頁）

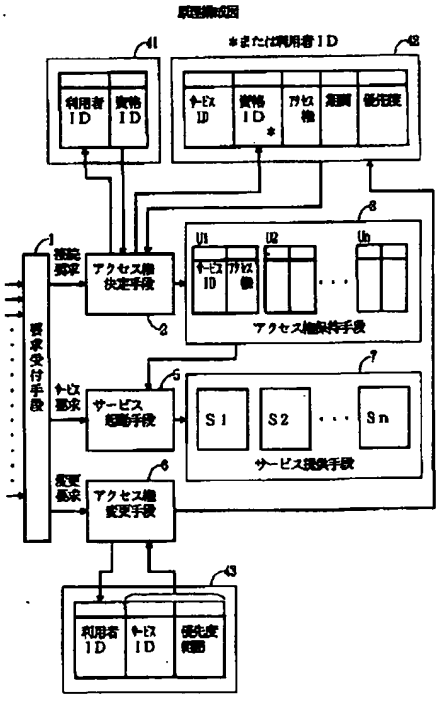
(21)出願番号　特願平6－32713

(22)出願日　平成６年(1994)３月３日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地
(72)発明者　大浦　雅彦
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(74)代理人　弁理士　井桁　貞一

(54)【発明の名称】　アクセス権管理装置

(57)【要約】
【目的】多数の利用者を対象に複数の情報処理サービスを提供する情報システムでの処理要求の妥当性を管理するアクセス権管理に関し、アクセス権の変更を柔軟に、管理を容易にする。
【構成】利用者ＩＤと資格ＩＤとを項目とするレコードを保持する利用者資格ファイル41と、サービスＩＤと、資格ＩＤまたは利用者ＩＤと、アクセスの種類と可否と、レコードの優先度とを項目とするレコードを保持するアクセス権ファイル42と、要求受付手段１と、アクセス権決定手段２と、アクセス権保持手段３と、サービス起動手段５とを有する。アクセス権決定手段２は、利用者ＩＤをキーとして利用者資格ファイル41から資格ＩＤを取り出し、資格ＩＤと利用者ＩＤをキーとしてアクセス権ファイル42を検索して、同一のサービスについて優先度の高いレコードにより最終的なアクセスの可否を決定しアクセス権保持手段３に保持する。



1

【特許請求の範囲】

【請求項1】　複数の利用者に対し複数の処理サービスを提供する情報システムにおける利用者のサービスへのアクセス権を管理する装置であって、

利用者資格ファイル（41）と、アクセス権ファイル（42）と、要求受付手段（1）と、アクセス権決定手段（2）と、アクセス権保持手段（3）と、サービス起動手段（5）とを有し、

利用者資格ファイル（41）は、利用者ＩＤと、その利用者のサービスへのアクセスに関する資格を表す資格ＩＤとを項目とするレコードを保持し、

アクセス権ファイル（42）は、サービスＩＤと、資格ＩＤまたは利用者ＩＤと、アクセスの種類とその可否と、そのレコードの優先度とを項目とするレコードを保持し、

要求受付手段（1）は、利用者からの要求を受付けて、接続要求をアクセス権決定手段（2）へ、サービス要求をサービス起動手段（5）へ伝え、

アクセス権決定手段（2）は、利用者からの接続要求があると、利用者ＩＤをキーとして利用者資格ファイル（41）を検索してその利用者ＩＤの存在の確認と、対応する資格ＩＤの取り出しとを行い、資格ＩＤおよび利用者ＩＤをキーとしてアクセス権ファイル（42）を検索して、同一のサービスについて複数のレコードがある場合には、優先度の高いレコードのアクセス権の指定により最終的なアクセスの可否を決定して、利用者ＩＤごとにサービスＩＤとアクセスの可否とをアクセス権保持手段（3）に保持し、

サービス起動手段（5）は、受け付けた利用者からのサービスへのアクセス要求があると、利用者ＩＤとサービスＩＤとアクセス種類とを受け取り、その内容が、アクセス権保持手段の内容に合致する場合に指定されたサービス提供手段を起動し、合致しなければ拒絶するように構成したアクセス権管理装置。

【請求項2】　アクセス権ファイル（42）は、サービスＩＤと、資格ＩＤまたは利用者ＩＤと、アクセスの種類とその可否と、そのレコードの優先度と、そのレコードの有効期間とを項目とするレコードを保持し、アクセス権決定手段（2）は、アクセス権ファイル（42）のレコードにより最終的なアクセスの可否を決定する場合に、有効期間外のレコードは無視することを特徴とする請求項1に記載のアクセス権管理装置。

【請求項3】　管理者情報ファイル（43）とアクセス権変更手段（6）とを設け、

管理者情報ファイル（43）には、アクセス権ファイル（42）の更新を行なう権限をもつ利用者の利用者ＩＤとサービスＩＤと優先度範囲とを項目とするレコードを保持し、

アクセス権変更手段（6）は、要求受付手段（1）からアクセス権ファイル（42）の内容の変更要求を受ける

2

と、管理者情報ファイル（43）を検索し、その利用者が設定可能なサービスと優先度範囲をチェックし、それを許可するか否かを決定することを特徴とする請求項1または請求項2に記載のアクセス権管理装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は多数の利用者を対象に複数の情報処理サービスを提供する情報システムに関する。特にその処理要求の妥当性を管理するアクセス権管理装置に関する。

【０００２】多数の利用者を対象に複数の情報処理サービスを提供する情報システムにおいては、サービスに対する要求（アクセスの種類・アクセス権）の管理・規制を行なっている。運用中に、利用者のアクセス権の変更・追加、特に一時的な変更や、サービスの追加・変更、特に一時的変更・試験的提供等の処理を行なうことが必要であり、それをシステムの安全性を損なわずに、かつ利用者の不便をきたさないように行なうことが要求されている。

【０００３】

【従来の技術】サービスには、例えば、電子伝票、会議室予約、旅費精算等の全員がアクセスできるものや、人事情報・評価のように特定の資格者のみアクセスできるものがある。

【０００４】サービスに対する要求の管理・規制の方法として、利用者個々に対して利用できるサービスとその処理内容（参照・更新等）や期間等を定義しておく方法が考えられるが、管理情報の量が膨大になるので、利用者の資格によるグループ設定を行い、このグループに対してアクセス権の内容を設定するやり方がある。グループはサービス毎に設定することができ、さらに、一般利用者、管理職、サービスの管理者あるいは処理の開発者等により分けることができる。

【０００５】予算申請を受け付けて登録するサービスのように、ある期間を設け、申請期限を過ぎてからの新規申請や申請データの修正は特定者以外には禁止する場合、従来の技術でも利用者の属するグループによるアクセス権の管理は実現可能である。ところで、そのサービスの管理者が、申請データを処理（例えば集計）する際に、申請データに誤りを発見し、その申請を行なった利用者に再申請を指示する必要がある場合を考える。このとき、申請期限は過ぎているので、他の利用者に対しては受け付けないようにする必要がある。従来の技術では、このような場合、その特定の利用者をその属するグループから一時的に外し、別のグループに（申請可能なグループ）に入れることになるが、特定の利用者は一時的に元のグループから外されるため、そのグループに許されていた他のサービスへのアクセスが制限されたり、逆に、本来制限されるはずのアクセスができてしまったりする可能性ができる。

【0006】

【発明が解決しようとする課題】従って、このような副作用を起こさないようにするには、この処理はかなり面倒な管理を必要とするものとなる。すなわち、関連するアクセス権情報を矛盾のないようにすべて修正し、さらに一時的な処置が済んだ時点で早急にもとに戻す必要がある。

【0007】本発明は、個々のアクセス権情報に優先度表示を付けて複数のアクセス権情報を同時に存在させ、優先度の高い情報によって実際のアクセス権を決定することにより、一時的な変更を含めてアクセス権の変更を柔軟にでき、かつ管理が容易なアクセス権管理装置を実現することを目的としている。

【0008】

【課題を解決するための手段】図1は本発明の原理構成図である。複数の利用者に対し複数の処理サービスを提供する情報システムにおける利用者のサービスへのアクセス権を管理する装置であって、第1の発明は、利用者資格ファイル41と、アクセス権ファイル42と、要求受付手段1と、アクセス権決定手段2と、アクセス権保持手段3と、サービス起動手段5とを有する。

【0009】利用者資格ファイル41は、利用者ＩＤと、その利用者のサービスへのアクセスに関する資格を表す資格ＩＤとを項目とするレコードを保持する。アクセス権ファイル42は、サービスＩＤと、資格ＩＤまたは利用者ＩＤと、アクセスの種類とその可否と、そのレコードの優先度とを項目とするレコードを保持する。

【0010】要求受付手段1は、利用者からの要求を受付けて、接続要求をアクセス権決定手段2へ、サービス要求をサービス起動手段5へ伝える。アクセス権決定手段2は、利用者からの接続要求があると、利用者ＩＤをキーとして利用者資格ファイル41を検索してその利用者ＩＤの存在の確認と、対応する資格ＩＤの取り出しとを行い、資格ＩＤおよび利用者ＩＤをキーとしてアクセス権ファイル42を検索して、同一のサービスについて複数のレコードがある場合には、優先度の高いレコードのアクセス権の指定により最終的なアクセスの可否を決定して、利用者ＩＤごとに、サービスＩＤとアクセスの可否とをアクセス権保持テーブルとしてアクセス権保持手段3に保持する。

【0011】サービス起動手段5は、受け付けた利用者からのサービスへのアクセス要求があると、利用者ＩＤとサービスＩＤとアクセス種類とを受け取り、その内容が、アクセス権保持テーブルの内容に合致する場合に指定されたサービス提供手段を起動し、合致しなければ拒絶する。

【0012】第2の発明は、アクセス権ファイル42は、サービスＩＤと、資格ＩＤまたは利用者ＩＤと、アクセスの種類とその可否と、そのレコードの優先度と、そのレコードの有効期間とを項目とするレコードを保持する。そして、アクセス権決定手段2は、アクセス権ファイル42のレコードにより最終的なアクセスの可否を決定する場合に、有効期間外のレコードは無視する。

【0013】第3の発明は、管理者情報ファイル43とアクセス権変更手段6とを設け、管理者情報ファイル43は、アクセス権ファイル42の更新を行なう権限をもつ利用者の利用者ＩＤとサービスＩＤと優先度範囲とを項目とするレコードを保持する。

【0014】アクセス権変更手段6は、要求受付手段1からアクセス権ファイル42の内容の変更要求を受けると、管理者情報ファイル43を検索し、その利用者が設定可能なサービスと優先度範囲をチェックし、それを許可するか否かを決定する。

【0015】

【作用】利用者が情報システムにログインしてきたとき、要求受付手段1は接続要求として利用者ＩＤ（例えばＵ1）をアクセス権決定手段に渡す。アクセス権決定手段2は、利用者ＩＤをキーとして利用者資格ファイル41を検索し、資格ＩＤを得る。さらに、資格ＩＤと、利用者ＩＤとをキーとしてアクセス権ファイル42を検索して、どちらかを含むレコードを抽出する。ここで、もし同一サービスに対するレコードが複数ある場合は、優先度の値が一番大きなレコードのアクセス可否項目をアクセス権として採用する。このようにしてサービスＩＤとアクセス権とを対応させたアクセス権保持テーブルを生成してアクセス権保持手段3に保持する。この対応テーブルは利用者ＩＤごとに区別しておく。利用者がログアウトした場合は、その利用者ＩＤのアクセス権保持テーブルは削除することになる。

【0016】利用者からのサービスＳ1へのアクセス要求を受けて、要求受付手段1は利用者ＩＤとサービスＩＤとをサービス起動手段5へ渡す。サービス起動手段5は、アクセス権保持手段に保持されたアクセス権保持テーブルを参照してアクセス可能と判断したらサービス提供手段の所定のサービスを起動する。

【0017】このように構成することにより、アクセス権ファイルには、同じサービスに対する同じ利用者の異なるアクセス権を指定したレコードが複数存在することになるが、どちらの指定を採るかが優先度によって決定され一意に定まる。従って、部分的に、または一時的にアクセス権を変更する場合に、変更したい内容にした（優先度の値は大きい）レコードを追加することができる。もとにもどす場合にはそれを削除するだけでよい。

【0018】第2の発明では、アクセス権を指定したレコードの有効期間を項目の1つにして指定してあるので、その期間外であれば、そのレコードは無いのと同じであり、前もって追加しておいたり、削除を延ばしたりしても問題がなく、アクセス権管理が容易になる。

【0019】第3の発明では、アクセス権ファイル42の内容更新を要求された場合には、更新要求者の利用者Ｉ

ＤをキーとしてＤ管理者情報43を検索し、該当する項目が存在しなければ、更新要求を拒絶し、存在するならば変更対象のサービスＩＤと設定可能な優先度の範囲を限度としてアクセス権の更新を許可する。従って、アクセス権の変更を適正に行なうことができる。

【００２０】

【実施例】以下、図面を参照して本発明の実施例を説明する。図２は本発明の一実施例の構成図である。図１と同一の機能のものは、同一の符号を付して示す。

【００２１】図２において、利用者用の端末装置91は回線90を通じて情報システム92に接続されている。情報システム92は、メモリ81、プロセサ82、ファイル装置83、通信制御装置84よりなる。メモリ81には、全体を制御するオペレーティングシステム70と、利用者から要求されたサービスを実行するサービスプログラム７と、図１の原理構成図に示したアクセス権管理のための手段を実現したプログラムとがある。アクセス権管理のための手段を実現したプログラムは、端末装置91から入力されたコマンドを受け付けたり、サービスの実行結果を端末装置91に表示する制御を行なう要求受付部１と、利用者毎のアクセス権を決定するアクセス権決定部２と、アクセス権のチェックを行なってサービスプログラムを起動するサービス起動部５と、アクセス権を変更するためのアクセス権変更部６とよりなる。

【００２２】利用者の情報を格納した利用者資格ファイル41と、各サービスのアクセス権情報を格納したアクセス権ファイル42と、アクセス権情報を管理する管理者の情報を格納した管理者情報ファイル43とはファイル装置83に保持され、利用者毎のアクセス権の内容を保持するアクセス権保持部３はメモリ81またはファイル装置に保持される。これらのファイルやテーブルの操作、端末装置91とのやり取り等はオペレーティングシステム70を通して行なうが、自明のこととして以下の説明では省略する。

【００２３】図３は本実施例のファイル構成図である。図３（１）は利用者資格ファイル41の構成を示す。各利用者には、利用者ＩＤ、パスワード、所属グループが定義してある。

【００２４】図３（２）は、アクセス権ファイル42の構成を示す。アクセス権情報はそれぞれ、対象となるサービス、グループ、処理（参照、更新毎の可否）、期間、優先度の各項目で構成されている。項目の値が‘ ALL ’の場合は、その項目についてはすべてが対象となることを示す。また、グループの項目には、グループＩＤ（資格ＩＤ）の他に、利用者ＩＤを設定することもできる。期間の項目は、そのアクセス権情報レコードが適用される期間を示している。優先度の項目は、同一サービス、同一利用者に対してレコードが複数あるとき数値が大きいレコードが優先して使用されることを示す。

【００２５】図３（３）は、管理者情報ファイル43の構成を示す。管理者情報ファイル43は、管理対象となるサービスのＩＤと、管理者の利用者ＩＤと設定可能な優先度の範囲を示す値が定義してある。

【００２６】情報システムのサービスの例として、本実施例では電子伝票Ｓ１、会議室予約Ｓ２、旅費精算Ｓ３等が提供されている。上記サービスを提供するため、サービスプログラム７は、各サービスを実現するプログラムモジュール（Ｓ１，Ｓ２，Ｓ３，・・・）から成り、各サービスはサービス起動部５によって対応するプログラムモジュールが起動されることによって行なわれる。

【００２７】以下に、本実施例の動作について説明する。まず利用者（ＩＤ：Ｕ１）は、端末装置91を操作して、接続要求をする。具体的には、端末装置91から利用者ＩＤとパスワードを入力する。すると要求受付部１は、入力された利用者のＩＤとパスワードの組を渡してアクセス権決定部２を起動する。アクセス権決定部２は利用者資格ファイル41から抽出した情報と照合して、もし、照合の結果が一致すれば接続要求を受理し、そうでなければ拒絶する。この段階はいわゆるログイン処理である。接続要求が受理された利用者については、以下の手順でアクセス権の調査が行なわれ、その結果がアクセス権保持テーブルとしてアクセス権保持部３に書き込まれ、その利用者が情報システム92との接続を開放（ログアウト）するまで保持される。そして、利用者からのサービスへのアクセス要求があるたびに、サービス起動部５は、このアクセス権保持テーブルの内容をチェックし、利用者が所望するサービスと処理に関するアクセス権が‘可’であれば、対応するプログラムモジュールを起動し、‘否’であれば利用できない旨のメッセージを端末装置91に送る処理を行なう。

【００２８】アクセス権保持部３への利用者のアクセス権の格納の手順を、図３、図４を参照しながら以下に説明する。アクセス権決定部３は、要求受付部１からの要求を受けてまず利用者資格ファイル41から利用者Ｕ１が所属するグループ（資格ＩＤ）を抽出する（この例ではＧ１とＧ３に属している）。

【００２９】次に、情報システムで提供されている各サービスについて以下の処理を行なう。サービスＳ１に対するアクセス権を求めるために、先ずアクセス権ファイル42から、サービスの値が‘ ALL ’または‘Ｓ１’であり、かつグループの値が‘ ALL ’または利用者Ｕ１が所属するグループ（Ｇ１，Ｇ３）または利用者のＩＤ（この場合Ｕ１）と一致するレコードで、期間の指定があればその期間内であるものを抽出し、優先度の値が最大であるレコードの値を各処理（更新、参照）ごとに求め、アクセス権保持部３に格納する。この操作をすべてのサービスについて繰り返す。

【００３０】図４（１）は、アクセス権ファイル42に、図３（２）のａ～ｃのレコードが登録され有効である場合（すなわちレコードｄがない場合または指定期間外）

に、アクセス権保持部3に格納される利用者ＩＤ＝Ｕ１の利用者に関する情報すなわちアクセス権保持テーブルの内容の例である。

【００３１】図４（２）は、アクセス権ファイル42に図３（２）のａ～ｄのレコードが登録され有効である場合（すなわちレコードｄがあり指定期間内の場合）に、アクセス権保持部３に格納される利用者ＩＤ＝Ｕ１の利用者に関する情報すなわちアクセス権保持テーブルの内容の例である。

【００３２】このアクセス権ファイルのレコードｄは、従来技術の項で述べた電子伝票の誤りを訂正するような場合に、利用者Ｕ１のみ更新できるように一時的に追加した項目であり、利用者Ｕ１が更新を完了したらこの項目を削除することにより、本来のアクセス権設定状態に戻すことができる。なお、削除しなくても指定期間外になれば自動的に無効になる。

【００３３】なお、図３（２）のアクセス権ファイルの内容を説明する。レコードａは、すべてのサービスをすべての利用者に開放することを意味する。このレコードだけであれば、なんの制約もなくアクセスできる。レコードｂが追加されると、サービスＳ１についてはグループＧ１とＧ２に属する利用者にのみ更新アクセスが期間を限って許されなくなる。レコードｃが追加されると、指定された期間の間は、それまで全員がアクセスできたサービスＳ３がアクセスできなくなる。これは例えば、サービスＳ３の内容の変更のため一時的にサービスを中止する場合である。レコードｄが追加された場合は、先に説明した通りである。

【００３４】一方、利用者が端末装置91からアクセス権ファイル42の更新を要求した場合、要求受付部１はアクセス権変更部６を起動する。アクセス権変更部６は、管理者情報ファイル43に、更新を要求している利用者ＩＤと更新を要求しているサービスＩＤの組が登録されていれば、そこに登録されている優先度の範囲でそのサービスについてのアクセス権管理情報のレコードをアクセス権ファイル42に追加・削除・更新を許可する。これにより、アクセス権の変更がみだりに行なわれたり、誤って他のサービスに影響するようなことを防ぐことができる。

【００３５】

【発明の効果】以上説明したように、情報システムの運用中にアクセス権の変更を柔軟にでき、かつ管理が容易なアクセス権管理装置を実現することができる。システムの安全性を損なわずに、かつ利用者の不便をきたさないように、利用者のアクセス権の変更・追加、特に一時的な変更や、サービスの追加・変更、特に一時的変更・試験的提供等の処理を行なうことができる。

【図面の簡単な説明】

【図１】　本発明の原理構成図

【図２】　本発明の実施例の構成図

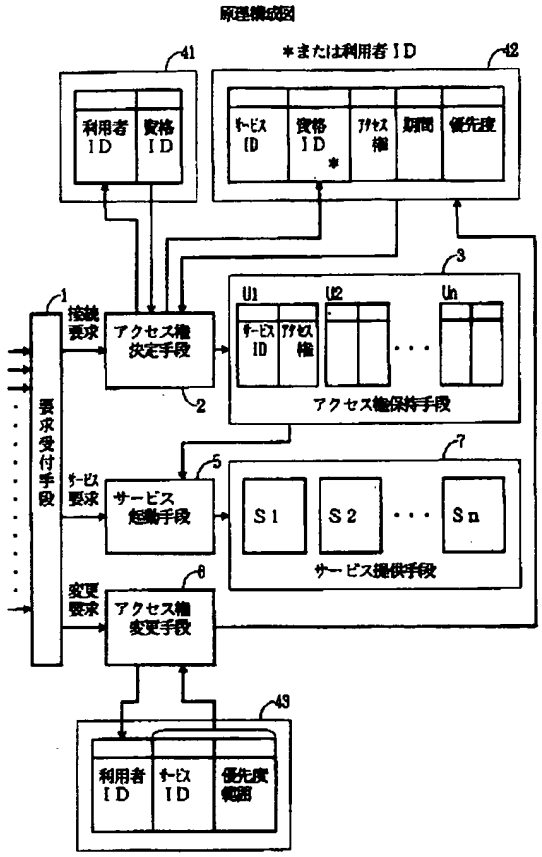
【図３】　実施例のファイル構成図

【図４】　アクセス権保持テーブルの内容の例

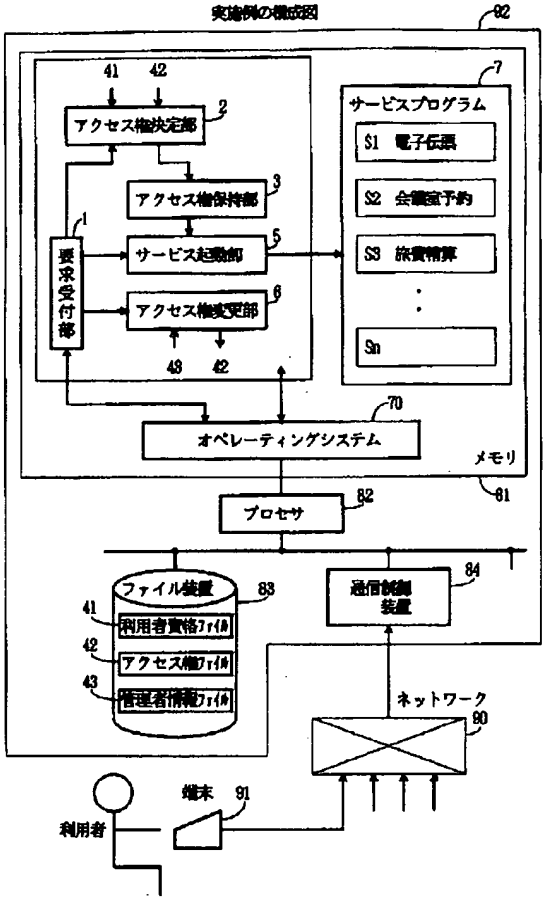
【符号の説明】

1　要求受付手段（要求受付部）
2　アクセス権決定手段（アクセス権決定部）
3　アクセス権保持手段（アクセス権保持部）
41　利用者資格ファイル
42　アクセス権ファイル
43　管理者情報ファイル
5　サービス起動手段（サービス起動部）
6　アクセス権変更手段（アクセス権変更部）
7　サービス提供手段（サービスプログラム）
70　オペレーティングシステム
81　メモリ
82　プロセサ
83　ファイル装置
84　通信制御装置
90　ネットワーク
91　端末装置
92　情報システム

【図1】



【図2】



【図4】

アクセス権保持テーブルの内容の例　（ID：U1の場合）

（1）レコードdがない場合または指定期間外の場合

サービス	参照	更新
S1	可	否
S2	可	可
S3	否	否
：		

（2）レコードdがあり指定期間内の場合

サービス	参照	更新
S1	可	可
S2	可	可
S3	否	否
：		

【図3】

実施例のファイル構成図

(1) 利用者資格ファイル

利用者ID	パスワード	グループ(資格)
U1	ABCD	G1, G3
U2	DEFG	G1, G2
U3	GHIJ	G1
M11	XYZA	G1, G10
・		

(2) アクセス権ファイル

	サービス	グループ	参照	更新	期間	優先度
a	ALL	ALL	可	可		10
b	S1	G1, G2		否	94/7/21 ～95/7/20	100
c	S3	ALL	否	否	94/7/20 ～94/7/22	50
d	S1	U1		可	94/7/21 ～94/7/21	200
	・					
	・					

(3) 管理者情報ファイル

サービス	利用者ID	優先度範囲
S1	M11	1～200
S2	M12, M13	1～100
S3	MS1	1～100
S3	MS2	1～500
・		
・		